BTEC Assignment Brief

Qualification	Pearson BTEC International Level 3 Diploma in Engineering Pearson BTEC International Level 3 Diploma in Electrical/Electronic Engineering Pearson BTEC International Level 3 Diploma in Digital Engineering Pearson BTEC International Level 3 Extended Diploma in Engineering Pearson BTEC International Level 3 Extended Diploma in Electrical/Electronic Engineering Pearson BTEC International Level 3 Extended Diploma in Digital Engineering Pearson BTEC International Level 3 Extended Diploma in Manufacturing Engineering
Unit number and title	**Unit 33: Computer Systems Security**
Learning aim(s)	**C:** Plan security measures to protect an engineering computer system from threats **D:** Implement security measures to protect an engineering computer system from threats
Assignment title	Protecting Computer Systems
Assessor	
Issue date	
Hand in deadline	

Vocational Scenario or Context	You have been hired as an apprentice IT Operations Technician at a small engineering firm specialising in computer aided manufacturing. The Managing Director of the company has tasked you with researching and upgrading the security of the computer system used for the storage of designs and specifications to bring it in line with the security used in their customer management web portal.

Task 1	Prepare a plan for the improvement of security to protect the engineering computer system from threats. Carry out the following analysis procedures on the current computer system: • Use tools and methods to assess the vulnerabilities, including port scanners, • Web vulnerability scanners • General vulnerability detection software • Audit of systems and network designs • Penetration testing for common threats in OWASP top 10 Perform risk assessments on the system for each possible threat, including giving a measure of its severity using an appropriate method of calculation. Justify how you reached your measure of severity for each risk, and suggest how they can be reduced. Identify the most severe risks and highlight them as a focus for your implementations. Updated security policies should form part of your plan, including analysis on methods of breaching the system and

	appropriate responses. Develop a test plan that can be used to check that your implementations were a success. Implement the security measures laid out in your plan. You should ensure all implementations are fully documented providing evidence of the before and after effects of the measure. Complete your test plan with results from performing the procedures carried out during the planning stage to ensure the improved security measures are a benefit to the system, suggesting further improvements to the system where appropriate. Evaluate how the improvements to the system are beneficial and have no major impact on the user.
Checklist of evidence required	A portfolio of evidence consisting of a report, screenshots, test results, witness statements, observation reports, analysis and planning documentation.

Criteria covered by this task:	
Unit/Criteria reference	To achieve the criteria you must show that you are able to:
33/D2	Optimise the effectiveness of the plan and of the protected engineering computer system safely, testing how well the system is protected by the measures and that users are not unreasonably hindered by the measures.
33/M3	Produce a detailed plan to protect an engineering computer system from possible threats, justifying the recommendations.
33/M4	Undertake security measures safely to fully protect severe vulnerabilities in an engineering computer system, testing how well the system is protected by the measures
33/P5	Produce a plan to protect an engineering computer system from possible threats.
33/P6	Undertake security measures safely to protect an engineering computer system.
33/P7	Test how well the engineering computer system is protected by the measures.